COT Security Alert – .NET Vulnerabilities

Multiple vulnerabilities have been reported in the Microsoft .NET Framework, specifically in ASP.NET, that could allow remote code execution. ASP.NET allows developers to build dynamic Web applications and Web services. Successful exploitation of some of the vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. One vulnerability could allow a denial of service attack.

Vulnerabilities:

- Collisions in Hash Table May Cause DoS Vulnerability
  Attackers may cause multiple collisions resulting in DoS. It is important to note that the hash collision attacks used to exploit this vulnerability does not only impact ASP.NET. This is an industry-wide issue affecting other Web Platforms, such as PHP and Ruby.

- Insecure Redirect in .NET Form Authentication Vulnerability
  An attacker could use a spoofing vulnerability to redirect users to a malicious website. Links in phishing emails could be utilized by attackers to direct users to the malicious site.

- ASP.Net Forms Authentication Bypass Vulnerability
  By using a known account name, an attacker could gain access and an elevation of privilege because of a vulnerability existing in the way that .NET Framework authenticates users. The attacker could then take any action within the ability of the targeted user, including executing arbitrary commands on the site.

- ASP.NET Forms Authentication Ticket Caching Vulnerability
  An attacker could gain elevation of privilege because of a vulnerability in how ASP.NET Framework handles cached content when Forms Authentication is used with sliding expiry. The attacker would need a victim to click on a link in an email or visit a malicious site for successful exploitation of this vulnerability. A successful exploitation of this vulnerability could allow the attacker to run commands with the ability of the currently signed-on user.

Microsoft has released Security Bulletin MS11-100 to address these vulnerabilities.

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/MS11-100
http://technet.microsoft.com/en-us/security/advisory/2659883

The following actions may be taken in response to this vulnerability:

- Apply the appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/